MILITARY HEALTH SYSTEM (MHS)		**IMPLEMENTATION GUIDE No. 13**	
INFORMATION ASSURANCE (IA) **IMPLEMENTATION GUIDE**		**EFFECTIVE DATE** 07/19/05	**REVISED DATE** xx/xx/xx

Subject:

INFORMATION ASSURANCE EDUCATION, TRAINING, AND AWARENESS

1 PURPOSE AND SCOPE

The provisions of this guide are policy for all TRICARE Management Activity (TMA) Components (TMA Directorates; TRICARE Regional Offices (TRO), and the Program Executive Office (PEO), Joint Medical Information Systems Office (JMISO)) (hereafter referred to as the TMA Component(s)). For TRICARE Contractors, this document is policy if required by contract; otherwise it serves as information assurance guidance. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate this document into their information assurance polices and procedures.

This implementation guide reaffirms DoD's Information Assurance (IA) training and awareness requirements for TMA Component personnel developing, using, operating, administering, maintaining, and retiring sensitive information (SI) on DoD ISs. This guide may be used to develop or enhance local training objectives and to assess training proficiency, in compliance with DoD Directive (DoDD) 8500.1, "Information Assurance (IA)," October 24, 2002, and DoDD 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004. The MHS approach is to focus on planning, executing, and assessing DoD requirement-based training while integrating a common training methodology across the MHS infrastructure to optimize training effectiveness and efficiency.

2 POLICY

It is MHS Policy that:

2.1 All TMA Component personnel and information technology (IT) users accessing a DoD IS receive initial IA awareness training during orientation as a condition of access and thereafter shall complete annual IA refresher awareness training. This shall include security reminders such as e-mail messages, newsletters, posters, etc. to increase security awareness.

2.2 Initial and annual IA awareness training shall ensure all TMA Component authorized users are familiar with local policies, incident reporting procedures, configuration management,

continuity of
operations plan, and disaster recovery.

2.3 IA education, training, and awareness shall be provided for all TMA military and civilian personnel, including contractors, commensurate with their respective responsibilities.

2.4 All MHS personnel and IT users are familiar with potential penalties for failure to comply with federal law.

2.5 Identify, document, track, and report IA personnel training, certifications, and certification status to the MHS CIO.

2.6 All TMA Component personnel and IT users shall comply with DoDD 8570.1.

3 PROCEDURES

3.1 Development and maintenance of an IT security training and awareness program for all TMA Component personnel is required in accordance with DoDD 8500.1.

3.2 Training programs shall be tailored to a user's need-to-know for secure operation or use of the system.

3.3 Initial and annual Privacy Act training shall be accomplished in accordance with DoD 5400.11-R, "DoD Privacy Program," for the protection of privacy information.

3.4 The following security areas, at a minimum, shall be addressed during training:

a. Workstation configuration and use.

b. Management of user identifications and passwords.

c. Avoidance and detection of computer viruses.

d. Contingency plans, disaster recovery, and procedures for continued operation during emergencies or system failures.

e. Detection, response, and reporting of IT security incidents.

f. Overview of IT security threats (sources and impacts) and vulnerabilities.

g. Computer viruses and other malicious code.

h. Password management.

i. Proper protection, storage, and disposal of SI.

j. Proper Internet usage.

k. Proper e-mail usage.

l. Software use, including awareness of copyright issues and software downloads from the Internet.

m. Area and physical security, including challenging strangers and escorting unauthorized personnel.

3.5 Security training and awareness can be accomplished using the following delivery methods:

a. Computer Based Training (CBT) via Defense Information Systems Agency's (DISA) Security Awareness compact disk (CD), or a comparable CBT course containing the same subject matter topics.

b. Pamphlets.

c. Classroom Instruction.

d. Placing security awareness training material on a network shared drive with the ability to track successful completion of training.

3.6 IA awareness and training is required for all authorized users before they are granted access to the system. Refresher training shall be conducted annually and when major system changes occur (e.g., a new operating system is installed).

3.7 A documented process for tracking and reporting training provided to all users, including the name of the person taking the course, title of course, dates of attendance, and cost shall be recorded to ensure compliance with requirements.

4 REFERENCES

a. CJCSM 6510.01, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)," March 25, 2003 (Change 1)

b. Defense Information Systems Agency (DISA), Information Assurance Support Environment (IASE) Web site – http://iase.disa.mil/eta

c. DoDD 5400.11, "DoD Privacy Program," December 13, 1999

d. DoD 5400.11-R, "Department of Defense Privacy Program," August 1983

e. DoDD 8500.1, "Information Assurance (IA)," October 24, 2002

f. DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003

g. DoDD 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004

h. NSTISSI 4013, "National Training Standard for System Administrators in Information Systems Security (INFOSEC)," March 2004

i. Federal Information Security Management Act of 2002

j. Health Insurance Portability and Accountability Act (HIPAA) Security Final Rule, February 20, 2003.

5 ACRONYMS

CBT	Computer Based Training
CD	Compact Disk
CND	Computer Network Defense
DISA	Defense Information Systems Agency
DoD	Department of Defense

DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
HIPAA	Health Insurance Portability and Accountability Act
IA	Information Assurance
IASE	Information Assurance Support Environment
INFOSEC	Information Security
IS	Information System
IT	Information Technology
JMISO	Joint Medical Information Systems Office
MHS	Military Health System
NSTISS	National Security Telecommunications and Information Systems Security
PEO	Program Executive Office
SI	Sensitive Information
TMA	TRICARE Management Activity
TRO	TRICARE Regional Offices